Die 6 Kategorien bekannter WLAN-Bedrohungen für Ihr Unternehmen und Möglichkeiten zum Schutz vor diesen Bedrohungen

WatchGuard

Inhalt

WLAN-Wachstum 3

Größere Angriffe auf WLANs 4

Die 6 Kategorien bekannter WLAN-Bedrohungen für Ihr Unternehmen 5

- Evil Twin Access Point 6
- Fehlerhaft konfigurierter Access Point 7
- Rogue Access Point 8
- Rogue Client 9
- Benachbarter Access Point 10
- Ad-hoc-Netzwerk 11

Trusted Wireless Environment zum Schutz vor WLAN-Bedrohungen 12

Marktführende Performance 13

Skalierbares Management 15

Verifizierte umfassende Sicherheit 17

WatchGuard: Sicheres, Cloud-managed WLAN 19

WLAN-Wachstum

Ein WLAN-Zugang ist zu einem normalen Bestandteil unseres Alltags geworden. Ob mobile Geräte, Notebooks und Videospiele oder auch Haushaltsprodukte: Nahezu alle Geräte sind auf eine WLAN-Verbindung angewiesen. Nach Einschätzung von Gartner wird die Zahl der vernetzten Geräte bis zum Jahr 2020 auf mehr als 20,4 Milliarden ansteigen.

Auch der Anteil der Smartphone-Nutzer ist enorm angestiegen. Waren es 2011 noch 35 %, so ist der Anteil 2018 auf 77 % gestiegen[1]. Kunden und Mitarbeiter, die ihre Smartphones und sonstigen WLAN-fähigen Geräte im Roaming-Betrieb nutzen, benötigen einen robusten WLAN-Zugang. Aber welche inhärenten Sicherheitsrisiken sind beim WLAN zu beachten? Haben Sie sich Gedanken über die Bedrohungen gemacht, die praktisch an jeder Ecke auf die Nutzer warten und bei denen es darum geht, die beim Herstellen der Verbindung gesendeten Informationen abzufangen?

Werfen wir einen Blick auf einen der größten Angriffe auf ein WLAN aus den letzten Jahren, von dem ein Unternehmen, ganz ähnlich zu Ihrem, betroffen war.

Nach Einschätzung von Gartner wird die Zahl der **vernetzten Geräte** bis zum Jahr **2020** auf **über 20,4 Milliarden** steigen.

1. https://www.securedgenetworks.com/blog/wi-fi-planning-preparing-for-growth-in-a-mobile-first-world

Größere Angriffe auf WLANs

TJ Maxx wurde im Juli 2005 Opfer einer Sicherheitsverletzung, die auf ein ungesichertes drahtloses Netzwerk zurückzuführen war. Der Hacker positionierte sich einfach mit einem Notebook und einer Teleskopantenne vor dem TJ Maxx-Standort in St. Paul (Minnesota). Dort lud er mindestens 45,7 Millionen Kredit- und Kundenkartennummern herunter. Potenziell hatte er jedoch Zugriff auf insgesamt bis zu 200 Millionen Kartennummern.[2]

Laut einem Bericht von CNBC vom Dezember 2017 hatte **Starbucks** die nötigen Schritte ergriffen, um zu verhindern, dass Kunden-Notebooks für die Erzeugung von Kryptowährung genutzt werden. Das WLAN in einer Filiale in Buenos Aires war gehackt und mit einem Spezialcode modifiziert worden. Sobald sich ein Nutzer am WLAN anmeldete, konnte der WLAN-Anbieter mit der Rechenleistung des Kundenrechners Bitcoins schürfen[3].

Im März 2018 wurden mehrere Beamte der Stadt Atlanta (USA) Opfer eines Ransomware-Angriffs, bei dem Dateien auf ihren Geräten verschlüsselt wurden. Um die Verbreitung von Ransomware über das WLAN zu verhindern, musste der internationale Flughafen Hartsfield-Jackson in Atlanta den Zugriff auf die eigenen WLAN-Services abstellen. Die schnelle Entscheidung des Sicherheitsteams in Atlanta schützte die Fluggäste vor einer potenziellen Infektion![4]

Vor welchen Bedrohungen müssen Sie Ihr Unternehmen schützen?

2. https://www.zdnet.com/article/tjxs-failure-to-secure-wi-fi-could-cost-1b/
3. https://www.cnbc.com/2017/12/12/starbucks-customer-laptops-hacked-to-mine-cryptocurrency.html
4. https://www.secplicity.org/2018/03/23/the-worlds-busiest-airport-shuts-off-wi-fi-amid-a-ransomware-attack/

Die 6 Kategorien bekannter WLAN-Bedrohungen für Ihr Unternehmen

Eine vollständige Liste potenzieller WLAN-Bedrohungen wäre praktisch unendlich. Es gibt jedoch 6 bekannte Bedrohungskategorien, vor denen Sie Ihr Unternehmen schützen müssen. Im nächsten Abschnitt gehen wir genauer auf die einzelnen Kategorien ein und klären die Frage, wie die Bedrohungen aussehen und funktionieren. Außerdem behandeln wir ein Beispiel, wie es sich so oder so ähnlich in Ihrem Unternehmen ereignen könnte.

Evil Twin Access Point

WAS

Ein Evil Twin Access Point (AP) imitiert einen legitimen AP, indem er seine SSID und eindeutige MAC-Adresse fälscht (Spoofing). Die Angreifer können anschließend den Datenverkehr abfangen und sich in die Datenkommunikation zwischen dem Opfer und den Servern, auf die das Opfer zugreift, einzuschalten, während das Opfer mit dem Evil Twin Access Point verbunden ist.

WIE

Sobald das Opfer die Verbindung hergestellt hat, kann der Angreifer Anmeldedaten stehlen, die Browser des Opfers mit bösartigem Code infizieren, das Opfer auf eine Malware-Site umleiten u. v. m.

BEISPIEL

Angenommen, Sie beschließen in der Mittagspause, dass es nun endlich an der Zeit ist, sich neu einzukleiden. Dagegen ist erst einmal nichts einzuwenden. Allerdings nutzt ein Hacker einen Evil Twin Access Point, weswegen Sie – ohne Verdacht zu schöpfen – eine Verbindung zu dessen Kopie Ihrer WLAN-SSID herstellen. Sobald Sie beim Bezahlvorgang Ihre Kreditkartendaten angeben, um das neue Kleidungsstück zu bestellen, kann der Hacker diese Informationen im Dark Web verkaufen.

Fehlerhaft konfigurierter Access Point

WAS

In stark frequentierten Netzwerken, in denen neue APs bereitgestellt werden, ist es nicht unüblich, dass Netzwerkadministratoren versehentlich Konfigurationsfehler begehen, wie z. B. das Öffnen einer privaten SSID ohne Verschlüsselung, wodurch sensible Informationen von Angreifern abgefangen werden könnten.

WIE

Dies kann jederzeit geschehen, wenn ein Access Point nicht richtig eingerichtet ist (wenn zum Beispiel die Standardeinstellungen unverändert bleiben).

BEISPIEL

Ein AP wird vom Unternehmen an die neue Niederlassung verschickt, und Charles von der Rezeption erklärt sich bereit, das Gerät einzurichten. Er befolgt die Anweisungen und installiert den AP, der eine offene SSID sendet und keinerlei private Daten zurückhält. Sie können ihm keinen Vorwurf machen, denn er ist kein IT-Experte. Dennoch existiert ein fehlerhaft konfigurierter AP, der ein schwerwiegendes Risiko für Ihr Unternehmen darstellen kann.

Rogue Access Point

WAS

Ein Rogue AP ist ein drahtloser Access Point, der ohne ausdrückliche Autorisierung eines Administrators in einem sicheren Netzwerk installiert wurde.

WIE

Rogue APs sind mit dem autorisierten Netzwerk verbunden, in der Regel mit einer offenen SSID, sodass Angreifer die Perimetersicherheit umgehen können. Bei einem Rogue AP kann es sich um einen physischen Access Point oder auch um einen per Software auf einem Computer erstellten und mit dem autorisierten Netzwerk verbundenen AP handeln.

BEISPIEL

In einem Einzelhandelsgeschäft gehen die Kunden den ganzen Tag ein und aus. Zu Stoßzeiten ist es unmöglich, alle Personen im Auge zu behalten. Jemand könnte sich ohne große Probleme Zutritt zum Technikraum verschaffen und dort einen Access Point anschließen, um auf das private sichere Netzwerk des Unternehmens zuzugreifen. Dadurch können POS-Systeme gekapert und Kreditkartennummern sowie andere vertrauliche Daten ausgelesen werden.

Rogue Client

WAS

Jeder Client, der zuvor mit einem Rogue AP oder einem anderen bösartigen AP in Reichweite eines privaten WLAN verbunden war, gilt als Rogue Client.

WIE

Ein Client fällt in der Regel in die Kategorie der Rogue Clients, sobald er eine Verbindung zu anderen Rogue APs, Evil Twins oder sonstigen APs hergestellt hat, während er sich in Reichweite eines privaten WLAN befand. Dieser Client könnte von einer Vielzahl von Man-in-the-Middle (MitM)-Angriffen betroffen sein, so z. B. Ransomware, Malware oder Backdoors zum Client.

BEISPIEL

Sie suchen jeden Tag auf dem Weg zur Arbeit dasselbe Café auf. Da Sie zuvor bereits einmal eine Verbindung zum WLAN des Cafés hergestellt hatten, stellt das Telefon die Verbindung automatisch wieder her, sobald Sie das Café betreten. Dummerweise hat jemand an diesem Tag einen Evil Twin AP eingerichtet und damit Ihr Smartphone überlistet. Während des Aufenthalts in Ihrem privaten WLAN wird das Smartphone mit Ransomware infiziert, die Sie mit ins Büro bringen. Sobald Sie am Schreibtisch sitzen, stellt das Smartphone eine Verbindung zum Firmen-WLAN her und verteilt damit die Ransomware im Unternehmen.

Benachbarter Access Point

WAS

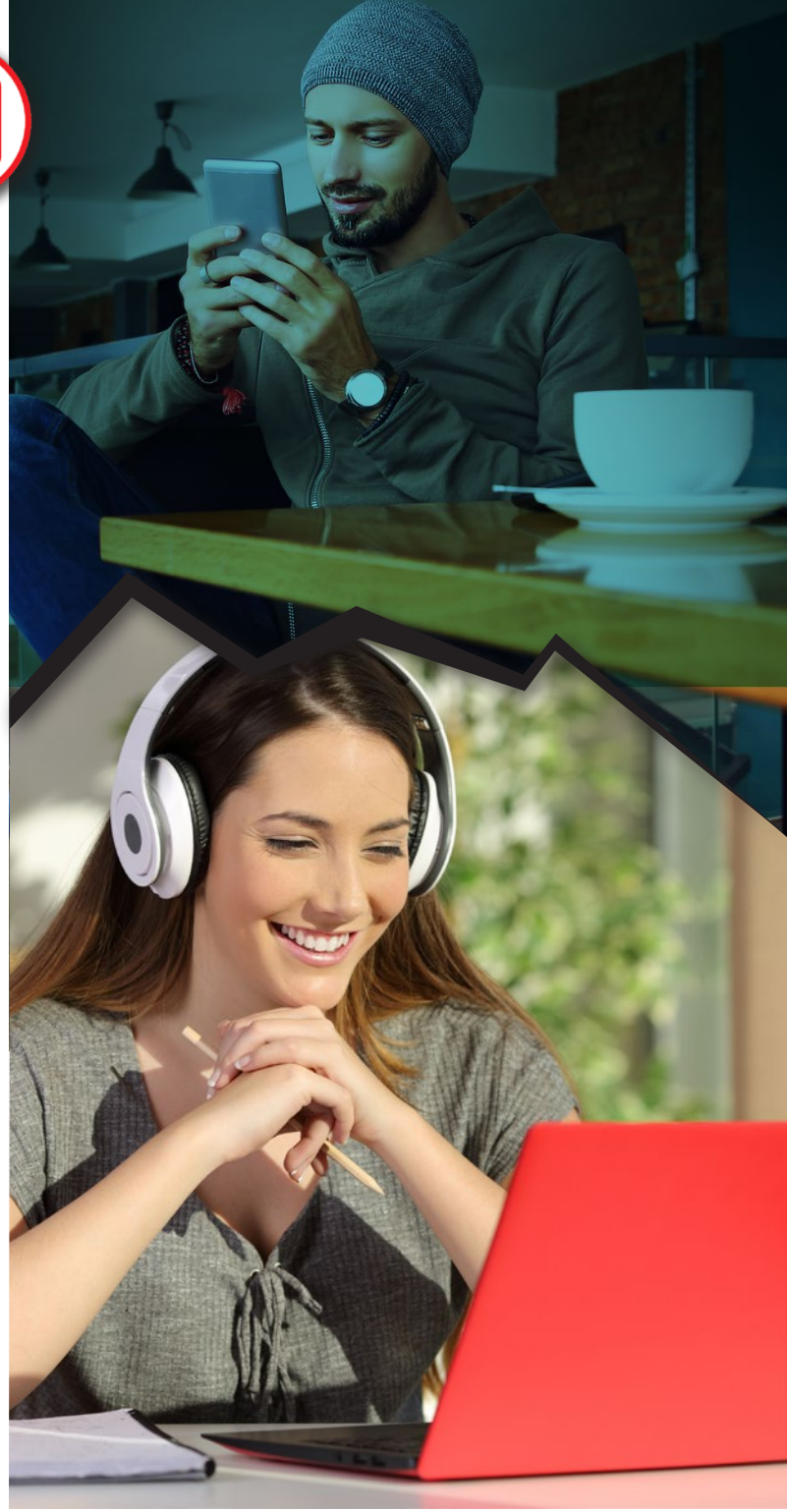
Von einem benachbarten AP ist die Rede, wenn ein autorisierter Client eine Verbindung zu einem Gast-AP oder einem externen, benachbarten AP herstellt und damit die Perimetersicherheit des Unternehmens sowie die Sicherheitsbeschränkungen der Firewall umgeht.

WIE

Für diese Bedrohung sind keine geheimen Hacking-Künste erforderlich. Jede Mitarbeiterin und jeder Mitarbeiter könnte die Bedrohung verursachen (und tut dies unter Umständen sogar). Durch die Herstellung einer Verbindung mit dem Gast-WLAN oder dem WLAN aus dem Café eine Etage tiefer umgehen die Mitarbeiter die in Ihrem Netzwerk vorgeschriebenen Sicherheitsmaßnahmen.

BEISPIEL

Janice aus der Marketingabteilung kann am frühen Morgen nicht auf ihre Lieblingsmusik verzichten. Ihr Telefonakku ist jedoch so gut wie leer, daher stellt sie über ihren Firmen-PC eine Verbindung zu einer Streaming-Site her. Die Firewall in ihrer Firma schränkt den Zugriff auf Musik-Streaming ein, aber das ist für Janice kein Problem. Sie stellt einfach eine Verbindung zum ungesicherten WLAN des Cafés eine Etage tiefer her. Unglücklicherweise wartet ein Hacker bei einer Tasse Kaffee genau darauf, dass Leute wie Janice eine Verbindung herstellen und darüber auch auf Ihr Netzwerk zugreifen.



Ad-hoc-Netzwerk

WAS

Eine Peer-to-Peer-WLAN-Verbindung zwischen Clients, bei der zwei oder mehr Geräte direkt miteinander kommunizieren und damit Ihre Richtlinien zur Netzwerksicherheit umgehen und den Datenverkehr vollkommen unsichtbar machen.

WIE

Mit einigen einfachen Klicks in den Einstellungen können die Mitarbeiter unkompliziert ein Ad-hoc-Netzwerk zwischen den Geräten der Kolleginnen und Kollegen einrichten. Dies hat sicherheitsrelevante und rechtliche Folgen, die sich letztlich auch auf das Geschäft auswirken können.

BEISPIEL

Zum Beginn einer Besprechung hat Karl eine Datei, die er seinem Chef allerspätestens für den Morgen versprochen hatte, IMMER NOCH nicht gesendet. Es würde zu lange dauern, die Datei nach der vom Unternehmen genehmigten Methode über das sichere Netzwerk freizugeben, also richtet er schnell ein Ad-hoc-Netzwerk ein und sendet die Datei direkt von Notebook zu Notebook. Unglücklicherweise öffnet diese Vorgehensweise Tür und Tor für potenzielle rechtliche und sicherheitsrelevante Konsequenzen für Ihr Unternehmen.

Trusted Wireless Environment zum Schutz vor WLAN-Bedrohungen

In einer Welt mit immer mehr offenen WLANs können Hacker nicht nur Informationen entwenden, sondern auch Malware auf Computern im Netzwerk verteilen und damit Schäden in Millionenhöhe verursachen. Sie benötigen einen Rahmen, innerhalb dessen Sie Ihren Kunden und Mitarbeitern ein Hochleistungs-WLAN bei höchster Sicherheit bereitstellen können.

Trusted Wireless Environment basiert auf den folgenden drei Säulen, um die gewünschte robuste Performance bei der benötigten Sicherheit zu ermöglichen:

1. **Marktführende Performance**
2. **Skalierbares Management**
3. **Verifizierte umfassende Sicherheit**

Lassen Sie uns jeder dieser Säulen und ihre Bedeutung für Unternehmen genauer betrachten.

Marktführende Performance 1

Gehen Sie in keine Kompromisse bei der Sicherheit ein, um das Performance-Niveau zu erreichen, das Sie für die Geschwindigkeit, Vernetzung und Clientdichte Ihrer WLAN-Umgebung benötigen. Wie wir bereits gesehen haben, kann ein langsames Unternehmens-WLAN eine einfache Ausrede für Mitarbeiter sein, die Verbindung zu einem weniger sicheren, aber schnelleren WLAN herzustellen.

Ein Hochleistungs-WLAN sorgt nicht nur dafür, dass die Mitarbeiter mit sicheren Netzwerken verbunden bleiben, sondern auch, dass sie mit maximaler Effizienz arbeiten können. Jede Unterbrechung, wie etwa beim Warten auf den Abschluss eines Ladevorgangs, ist eine Gelegenheit zur Ablenkung.

Die Mitarbeiter spielen in der Zwischenzeit auf ihrem Telefon herum oder drehen eine Runde durchs Büro.

Je nach Unternehmen kann ein Hochleistungs-WLAN den Unterschied zwischen zufriedenen Kunden und einer schlechten Bewertung in einem Internetforum ausmachen. In Restaurants, Hotels und sogar Arztpraxen wollen sich Kunden bzw. Patienten, die eine große zeitliche (und oft auch finanzielle) Investition beabsichtigen, darauf verlassen können, dass sie das WLAN nicht im Stich lässt. Eine langsame Verbindung oder ein schlechter Empfang treibt die Nutzer in die Arme der Konkurrenz – da kann Ihr Produktangebot noch so gut sein.

Ein Hochleistungs-WLAN sorgt nicht nur dafür, dass die Mitarbeiter **mit sicheren Netzwerken verbunden** bleiben, sondern auch, dass sie **mit maximaler Effizienz arbeiten** können.

Warum WatchGuard?

1

Die Zuverlässigkeit der Performance Ihrer drahtlosen Verbindung sollte Ihnen keine schlaflosen Nächte bereiten, sondern Tag für Tag eine Selbstverständlichkeit sein.

Die WatchGuard Secure Wi-Fi Cloud-Managementplattform und Access Points auf dem neuesten Stand der Technik, sorgen für die Performance, die Sie für Ihr Unternehmen benötigen. Unsere Access Point-Modelle sind so konzipiert, dass sie Umgebungen mit mittlerer Dichte – wie Schulen, verteilte Büroräume, Ladenlokale, Besprechungsräume, Restaurants oder Arztpraxen – ebenso unterstützen wie Umgebungen mit hoher Dichte wie etwa große Universitätscampus, Konferenzzentren und Einkaufszentren.

Darüber hinaus können unsere Access Points dank Mehrbenutzer-MIMO (MU-MIMO) mehrere nachgeschaltete Client-Geräte parallel unterstützen. Dadurch sinkt die Zeit, die die einzelnen Geräte bis zu einer Übertragung vom Access Point warten müssen, und die Netzwerkgeschwindigkeit steigt.

Das Beste dabei ist jedoch, dass Sie den Zugriff auf dieses Hochleistungs-WLAN Ihren Mitarbeitern und Kunden anbieten können, ohne ihre Sicherheitseinstellungen zurücknehmen zu müssen. Volle WLAN-Sicherheit bei voller WLAN-Performance – ein Gewinn für alle Beteiligten!

Die WatchGuard Secure Wi-Fi Cloud-Managementplattform und Access Points auf dem neuesten Stand der Technik sorgen für die **Performance, die Sie für Ihr Unternehmen benötigen.**

Skalierbares Management 2

Eine herausragende WLAN-Lösung, die sich jedoch nur schwer verwalten lässt, hilft weder bei der Sicherheit noch beim Betrieb der WLAN-Verbindungen eines Unternehmens. Sie benötigen eine Lösung, die einfach einzurichten und zu verwalten ist, damit Sie in der Lage sind, Ihr gesamtes WLAN, unabhängig von der Größe, über eine einzige Schnittstelle zu steuern und wichtige Prozesse zum Schutz von Umgebung und Benutzern auszuführen.

Sobald das Unternehmen wächst, sollte die WLAN-Bereitstellung problemlos mitwachsen. Die Zentralisierung des WLAN-Managements ermöglicht Unternehmen eine einfache Skalierung von einem einzelnen Wireless Access Point bis hin zu einer unbegrenzten Anzahl von Access Points an mehreren Standorten – ganz ohne Controller-Infrastruktur.

In einer Welt, in der WLANs allgegenwärtig sind, benötigen Sie außerdem die Visualisierung wichtiger Informationen wie Signalstärken-Reichweite, Bandbreitenverbrauch des WLAN-Client, Nutzung von Access Points, Applikationen und Client-Verteilung, damit stets der vollständige Überblick über das Unternehmen gewährt wird. Wenn Sie in der Lage sind, diese Daten visuell aufzubereiten und individuell anpassbare Berichte zu diesen Daten zu erzeugen, dann können Sie sich einen genauen Überblick über Ihr Unternehmen verschaffen, ohne stundenlang Zahlen auf einem Dashboard studieren zu müssen.

Die Zentralisierung des WLAN-Managements ermöglicht Ihrem Unternehmen eine einfache Skalierung von einem einzelnen Wireless Access Point bis hin zu einer unbegrenzten Anzahl von Access Points an mehreren Standorten – ganz ohne Controller-Infrastruktur.

Warum WatchGuard?

2

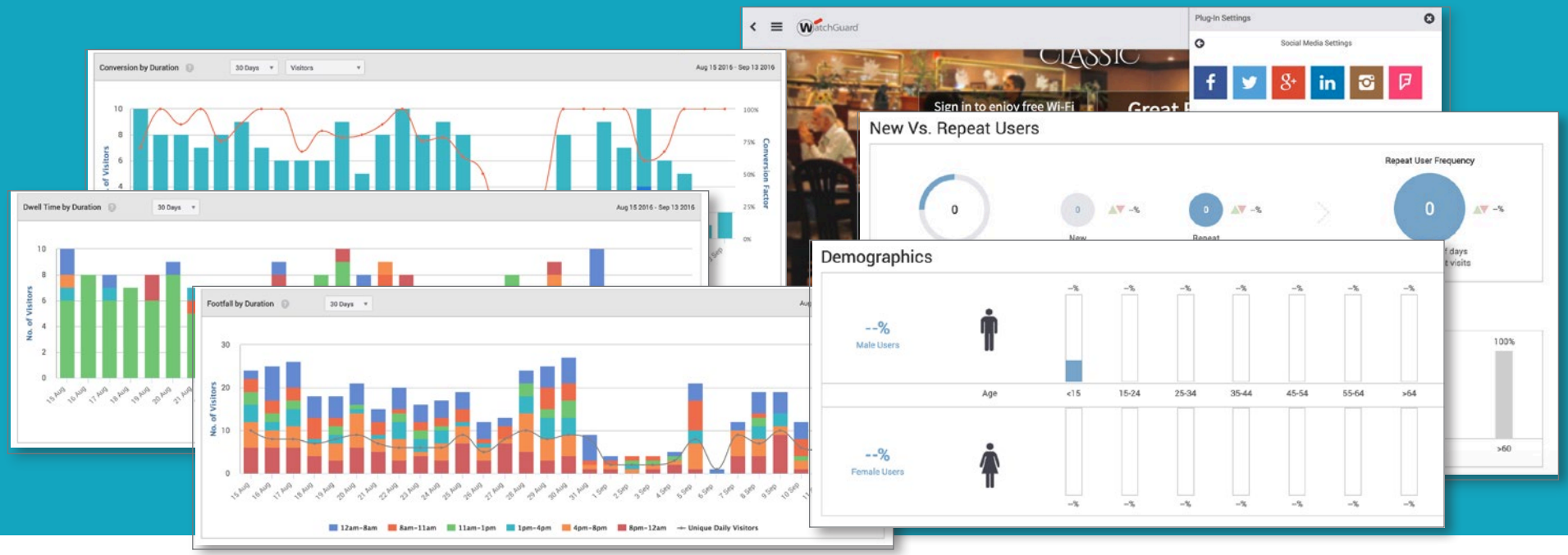
Die Wi-Fi-Cloud lässt sich problemlos einrichten und verwalten und ermöglicht die Kontrolle des gesamten WLAN von einer einzigen Schnittstelle aus. Gleichzeitig können Access Points nach den praktischsten Kriterien gruppiert werden, etwa nach Standort, Gebäude, Etage oder (im Fall eines Anbieters von Managed Services) sogar Kunde.

In der Wi-Fi Cloud von WatchGuard können Berichte, Dashboard Widgets, Konfigurationsvorlagen und verschiedene Analysedaten angezeigt werden. Administratoren können problemlos unbegrenzt verschachtelte Ordner für Gebäude, Etagen oder Gruppen erstellen und dabei Transparenz für den Ordner als Ganzes herstellen oder nur die Analysedaten für eine bestimmte Ebene freigeben.

Sie erhalten auch Einblicke in Anwendungen, die im WLAN-Netz im Einsatz sind. Durch das Monitoring und Reporting von mehr als 1.300 Anwendungen des Layer 2 und höher (wie Facebook, YouTube, Instagram usw.) können Sie eine Richtlinie zur fairen Nutzung anordnen und Netzwerküberlastungen auf ein Minimum beschränken.

Bleiben Sie außerdem im Hinblick auf Ihre WLAN-Umgebung stets auf dem neuesten Stand. Hierfür sorgen vordefinierte und anpassbare Vorlagen für die automatisierte Berichterstattung zu WLAN-Bedrohungen, Clientbestand, Compliancestatus und Performance. Dank der leistungsstarken Reporting-Engine der Wi-Fi Cloud können Sie Berichte planen und automatisch den gewünschten E-Mail-Empfängern zustellen.

In der **Wi-Fi Cloud von WatchGuard** können Sie **Berichte, Dashboard Widgets, Konfigurationsvorlagen** und **verschiedene Analysedaten anzeigen.**



Verifizierte umfassende Sicherheit 3

Zahlreiche aktuelle Wi-Fi-Anbieter begnügen sich bei der Bereitstellung von sicheren WLAN-Lösungen mit schwammigen Versprechen. Wie bei jeder Komponente zum Schutz Ihres Unternehmens benötigen Sie einen Nachweis dafür, dass die Lösung Ihr Unternehmen tatsächlich vor Angriffen über das WLAN schützt.

Eine wirklich umfassende Sicherheitslösung bietet zentrale Vorteile in den folgenden drei Bereichen:

- Automatischer Schutz vor den weiter oben erläuterten 6 Kategorien bekannter WLAN-Bedrohungen
- Möglichkeit des Betriebs legitimer externer Access Points in derselben Umgebung
- Beschränkung der Möglichkeit, dass Nutzer eine Verbindung zu nicht zugelassenen WLAN Access Points herstellen können

Diese Art von Daten rund um das Thema Sicherheit lassen sich bei den meisten wichtigen WLAN-Anbietern nur schwer herausfinden. Dies liegt offenbar daran, dass die Effektivität von Sicherheitslösungen in WLAN-Systemen noch nie getestet wurde. Bislang.

In einer kürzlich erstmalig durchgeführten Testreihe hat der Test- und Zertifizierungsanbieter Miercom einige der besten Access Points auf den Prüfstand gestellt: Die Geräte mussten Echtzeitanwendungen unterstützen und gleichzeitig gängige WLAN-Sicherheitsbedrohungen erkennen und verhindern. Die Tests umfassten die 6 Kategorien bekannter WLAN-Bedrohungen. Miercom zeichnete bei den Tests auf, wie lange es dauerte, bis die Bedrohung erkannt UND verhindert wurde.

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Test	Erkennung	Prävention	Erkennung	Prävention	Erkennung	Prävention	Erkennung	Prävention
Rogue-AP	P	P	F	–	F	MP	F	–
Rogue-Client	P	P	F	–	F	MP	–	MP
Benachbarter AP	P	P	P	P	F	–	F	–
Ad-hoc-Netzwerk	P	P	F	–	F	–	P	–
„Evil Twin" AP	P	P	P	F	P	MP	P	F
Fehlerhaft konfigurierter AP	P	P	P	–	–	–	–	–
Gleichzeitige Bedrohungen	P	P	F	F	F	F	F	F

P = Pass (Bestanden)
F = Fail (Nicht bestanden)
MP = Marginal Pass (Knapp bestanden)
– = Funktion nicht unterstützt

Den vollständigen Miercom-Bericht finden Sie hier: **www.watchguard.com/wifi-security-report**

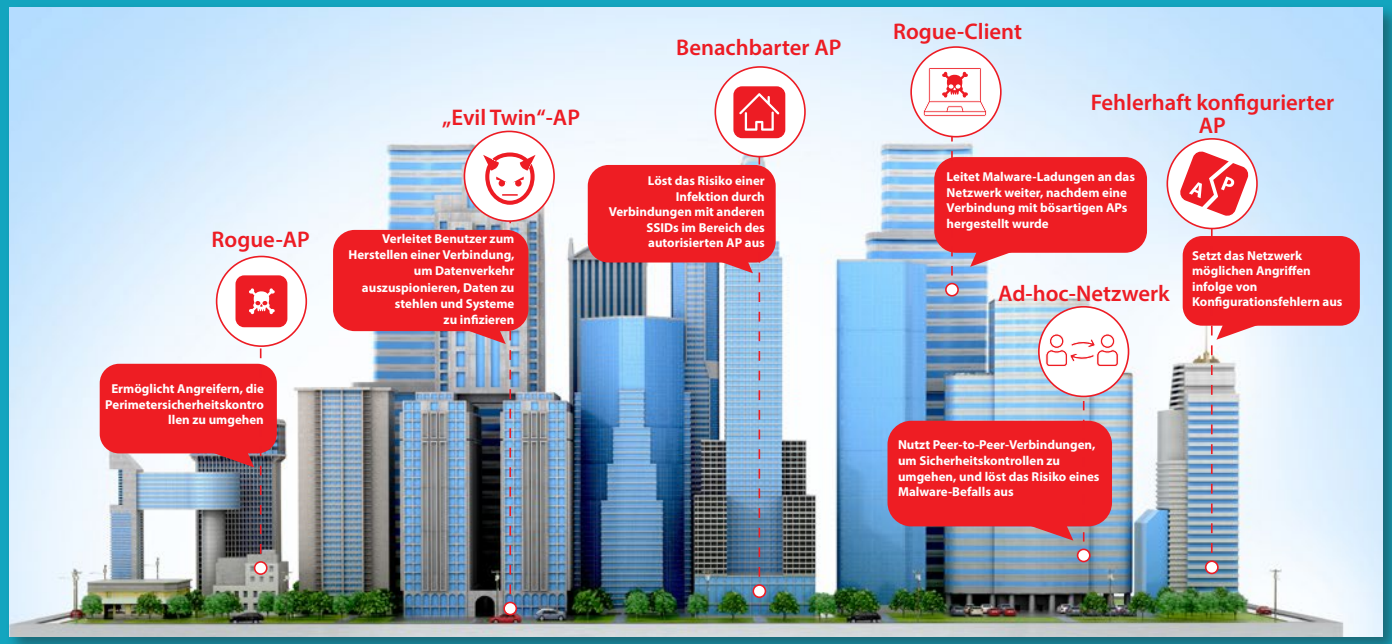
Warum WatchGuard? 3

WatchGuard ist der EINZIGE Anbieter, der die 6 bekannten Kategorien von WLAN-Bedrohungen nicht nur erkennt, sondern auch automatisch verhindert. Die WLAN-Lösung von WatchGuard war auch die einzige Lösung, die alle Bedrohungen in unter 20 Sekunden gleichzeitig erkennt und verhindert.

Unser patentiertes Wireless Intrusion Prevention System (WIPS) ist nicht mit anderen WLAN-Sicherheitslösungen auf dem Markt vergleichbar. Es sorgt für einen realen, genauen und automatisierten WLAN-Schutz für Ihr Unternehmen. Andere Anbieter setzen auf Signaturen und in erheblichem Maße auf Korrelationsregeln für MAC-Adressen. Dies kann zu einem hohen Anteil von False-Positive-Befunden führen. Unsere Marker Packet-Technologie schützt Ihr WLAN praktisch ohne False-Positives.

WatchGuard WIPS ist die einzige Lösung auf dem Markt, die alle Access Points und Clients in der Umgebung scannt und als autorisierte, externe oder Rogue APs klassifiziert. Durch die schnelle und zuverlässige Differenzierung zwischen den Access Points und Clients können Sie dafür sorgen, dass autorisierte APs und Clients den nötigen Zugriff erhalten, externe APs und Clients nicht eingebunden werden und Rogue APs und Clients keine Verbindung herstellen können.

WatchGuard ist der **EINZIGE Anbieter**, der die 6 bekannten Kategorien von WLAN-Bedrohungen nicht nur **erkennt**, sondern auch **automatisch verhindert**.



Die EINZIGE Wahl für Trusted Wireless Environments

WatchGuard ist der einzige Anbieter von Technologien und Lösungen für den Aufbau einer umfassenden Trusted Wireless Environment-Umgebung, die alle drei Kernanforderungen erfüllt – marktführende Performance, skalierbares Management und verifizierte umfassende Sicherheit – und Schutz vor allen 6 bekannten Kategorien von WLAN-Bedrohungen bietet.
Bei verschiedenen Tests kristallisiert sich WatchGuard als die einzige Lösung heraus.

Laut Miercom-Bericht konnte WatchGuard als EINZIGER Anbieter bei den folgenden Punkten überzeugen:

- Automatische und gleichzeitige Erkennung und Verhinderung der 6 Kategorien bekannter WLAN-Bedrohungen ohne Rückgang bei der WLAN-Performance
- Automatische Erkennung von Rogue APs und Rogue Clients und entsprechende Prävention
- Automatische Erkennung und Verhinderung von Endpunkten bei der Kommunikation über eine Ad-hoc-WLAN-Verbindung
- Automatische Verhinderung von Verbindungen zu „Evil Twin"-APs und gefährlichen Verbindungen zu fehlerhaft konfigurierten APs wie privaten SSIDs ohne Verschlüsselung

Erfahren Sie, wie Sie mit WatchGuard noch heute Ihre Trusted Wireless Environment aufbauen können!

Watchguard.com/trustedwirelessenvironment

DAS WATCHGUARD-SICHERHEITSPORTFOLIO

Netzwerksicherheit

Unsere Plattform stellt nicht nur Sicherheit auf Enterprise-Niveau bereit, sondern ist von Grund auf so konzipiert, dass der Fokus auf einer einfachen Bereitstellung, Verwendung und fortlaufenden Verwaltung liegt. Dies macht WatchGuard zur idealen Lösung für KMUs, mittelständische Unternehmen und dezentrale Großkonzerne weltweit.

Secure Wi-Fi

Die Secure Wi-Fi Solution von WatchGuard ist eine richtungsweisende Neuerung für den Markt von heute: Sie schafft eine sichere, geschützte WLAN-Umgebung, eliminiert den Verwaltungsaufwand und ermöglicht beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.

Multifaktor-Authentifizierung

Mit WatchGuard AuthPoint™ können Sie die Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach schließen. Beim einzigartigen Ansatz von WatchGuard wird die „DNA des Smartphones“ als Identifizierungsfaktor genutzt. Auf diese Weise wird sichergestellt, dass nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen erhält.

Mehr erfahren

Weitere Details erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter **www.trustedwirelessenvironment.com**.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für kleine und mittlere sowie dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.

Vertrieb Nordamerika: 1.800.734.9905 • Vertrieb in Deutschland, Österreich und der Schweiz: +49 700 92229333 • Web: www.watchguard.com/wifi

Mit diesem Dokument werden keine ausdrücklichen oder implizierten Gewährleistungen gegeben. Änderungen vorbehalten. Zukünftige Produkte, Funktionen oder Funktionalitäten werden zur Verfügung gestellt, sofern und sobald sie verfügbar sind. ®2018 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo und AuthPoint sind Marken bzw. eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr. WGCE67130_092118